



Running a network no longer means simply installing computers and keeping them going. Nowadays, security is an ongoing process, like backups and upgrades. Yet for many it remains shrouded in mystery. It's hard to establish a high level of network security, and harder still to ensure that the level of security stays high.

Hacking – the act of breaking into people's computers and networks – is on the rise. You may ask why a hacker would bother with your network when bigger prizes await elsewhere. It may be that the hacker wants a safe haven from which to launch a larger attack. But the trail of destruction ends at your network. And if you have no proper defences, there may be some embarrassing questions asked of you by law enforcement agencies.

Learning some of the hacker's tricks can help you discover your network's weaknesses and so correct them. In doing so, you could make a would-be attacker think twice before hacking you. If this sounds technical, though, don't worry. There are professionals who will analyse security on your network for you, and programs that will attempt to carry out the task automatically.

HACK ATTACK

Let's take a typical hacker. Before he attacks, he needs to know what internet-facing computers the target owns. For this he can look up its details on a

As computer networks become more powerful they also become more vulnerable to attack from hackers. But if you understand how hackers operate, you stand a better chance of outsmarting them. Jon Thompson explains how testing your network for weaknesses makes it stronger

local domain name system (DNS) server. The internet relies on DNS to translate automatically between host names and Internet Protocol (IP) addresses. But DNS can also provide a wealth of information that is useful to an attacker. If you have a machine called 'mail', for instance, it's likely that it's a mail server. Knowing this, our hacker can tailor his attack without first having to probe that system directly.

Another free information-gathering technique is to send an email to a deliberately badly spelt username at your domain. By default, most mail servers will respond with an automatic reply. This contains detailed information about the path taken to the target mail server, often including the operating system and mail software running, plus external and sometimes internal IP addresses. This helps our hacker to tailor further his eventual attack. So it is a good idea to tell your mail server to discard any undelivered email quietly.

Running your own web server may give you complete control over the hardware and software,

but legitimate requests can return information about the server, any running extensions and layered products and, if the software has not been updated, any security holes. Automated, free web server analysis tools such as Whisker and Nikto will find these holes quickly (see www.securiteam.com/tools/5XP040A6AK.html for details).

ON THE MAP

Techniques such as these can produce intricately detailed maps of networks for use in preparation for an attack. A good example of just how much information can be gathered in this way is shown in the 'Hacking the CIA' box opposite, detailing how UK security firm Matta legally produced a detailed map of some of the CIA's networks. There are other techniques, too, including 'dumpster diving', where hackers ransack bins for snippets of information. For many companies, a growing problem is that of hackers calling users and pretending to be from the service desk to dupe them into changing or revealing their passwords.



The typical hacker will spend considerable time looking for every source of network information. Providing contact email addresses on a website may seem like a great idea, but this can give our hacker one half of the username and password pairing he needs to log on. Statistically, there's a high probability that many passwords are simple variations on the username, a Premiership football team or something on the desk when the user thought of the password. For this reason, it's best to use an anonymous email account called, for example, enquiries@domain.com that handles contact with the public. Just don't make the password 'enquiries' too.

Other sources of seemingly innocent information can aid a hacker in mapping your network. Have you ever had a problem with a piece of software that you simply couldn't solve? If so, you may have asked for help in an online forum. You may have disclosed details of the troublesome computer and its configuration, or even how it fits into your network. Not all readers of such forums are friendly and eager to help. Be wary of people who ask for further details of your network.

Once he has a detailed view of your network, our hacker's next step might be to scan for open ports on the computers he knows about. It's dangerous for him to scan all 65,535 possible ports, because of the threat from any lurking intrusion-detection systems. He may instead test for single ports by connecting to them directly. See our 'Any Port in a Storm' box on page 220 for some well-known, regularly hacked ports and the services they carry. These should never be open to the internet, so block them at your firewall. Port scanning can be a problem for your firewall, too. By default, some have telltale patterns of ports that are dedicated to management functions. These can be visible to the outside world if you're not careful.

HOLE TRUTH

Our hacker may use any of a number of utilities to gently interrogate the TCP/IP stack on the servers he has identified. This can give enough information to tell him what operating system each server runs, down to its patch level, so it pays to keep updated.

There exists a vast arsenal of techniques for doing this. It pays to shore up your defences by discovering the holes in your security before a hacker finds them for you. There are plenty of tools and online services available to enable you to do this, and some have become industry standards.

One useful service used to extract server and update information from websites is the What's This Site Running? service provided by Netcraft at <http://news.netcraft.com>. Entering Microsoft, for instance, reveals that at the time of writing it was running Internet Information Server 6.0 on Windows Server 2003 with its last update being on 10th September 2004. If a hacker finds that you have an older version of a web server than the current release, or that you've not updated it, he can search for known hacking tools that will let him break in. These are known as exploits

Another useful website and tool is SamSpade (www.samspace.org). This allows you to gather information about your internet presence. Domain registration details, for instance, give names and sometimes email addresses that might prove useful, and can indicate whether an organisation has one or several physical sites. Some companies, growing through acquisitions, find that standards of

HACKING THE CIA

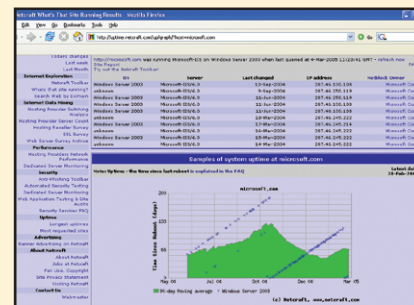
In 2002, London-based Matta Security Limited (www.trustmatta.com) showed just how important snippets of public information are when mapping a network in preparation for an attack. It chose its target well: the US Central Intelligence Agency, otherwise known as the CIA. The results make for sobering reading. To see them visit www.voelspriet.nl/Matta_Counterintelligence.pdf.

Using Google, Matta found the domains owned by the CIA and ran a search on the domain name system (DNS). This recovered several primary blocks of Internet Protocol (IP) addresses and a few secondary ones too. It then accessed the public domain registration records for its target at www.nic.gov. This provided information such as email addresses and names, plus a few more PC names and their associated IP addresses.

A zone transfer is a list of all the IP addresses and associated host names for a domain. Many DNS servers allow anyone to perform a zone transfer. At the time, the CIA's DNS servers were no exception. This revealed a lot of hosts, including web servers, mail servers and even a few internal IP addresses. It also allowed Matta to identify a few sub-domains, and this revealed still more computers.

Analysis of the data gathered at this point indicated that the names of various computers gave away their function, their operating systems and, in the case of routers, the make and model too. But there was worse to come.

Using Google, Matta managed to uncover full names, email addresses and phone numbers for dozens of CIA staff, as well as the



Such sites as Netcraft.com provide a wealth of web server information without the hacker needing to visit the target server himself

names and phone numbers of various departments, including the director's office.

A favourite hacker trick is to send an email to a target, with an address known not to exist. The resulting reply contains a large amount of diagnostic information including the path the message took through the internet and the target's network to get to the mail server and back. Used against the CIA, this could reveal information about the systems used and the way in which the already identified networks were connected.

Netcraft's What's This Site Running service provided additional information about the Agency's web servers, the software they ran and when they were last updated.

Putting this information together enabled Matta to produce a finished map of the CIA's networks (www.trustmatta.com/services/docs/cia-map.jpg) without the agency knowing and without breaking any laws or tripping any intrusion detection systems.



Nmap, used by security professionals and hackers alike, is a powerful port scanner, operating system identifier and host detection system

network security vary across the group. Our hacker can exploit these discrepancies. Part of the process of taking over a new company should include harmonising security across the network.

Another important network security tool is nmap, which is bundled with most mainstream Linux distributions. This tool, which combines a flexible port scanner, operating system identifier and host detection system, is useful for testing your systems for open ports and ensuring your firewall configuration prevents port scans. Further information, downloads and full documentation can be found at www.insecure.org/nmap.

Route tracing is an important technique for mapping the structure of a network. Most

operating systems contain a utility to do this. Linux calls it traceroute; Windows calls it tracert (see www.traceroute.org). These commands send a packet of information to a target server but the packet has a value called the time to live (TTL) that's set to expire as the packet hits the first computer on the route. When this happens, the PC or router that handled it when it expired sends a message back to your computer along with its own IP address. The utility then sends a second packet, this time with the TTL increased by one. The next computer on the path to the target responds with a message saying the packet has expired.

The route-tracing utility keeps sending out packets with increasingly large TTLs until it receives no response – possibly because of filtering by an internet service provider (ISP) – or the returned address is that of the target server. This is useful for tracing connection problems on large networks, but is just one of several information-gathering techniques that hackers use.

The most powerful hacking technique is to pretend to be a legitimate user. For this, a username and password combination is all that's needed. Finding the password to fit a known username is a skill akin to solving cryptic crosswords and many hackers spend years refining it. But there are password-cracking tools that show you which users have weak or easily guessed passwords.



ANY PORT IN A STORM

There are 65,535 possible ports, each associated with its own unique service. To maintain network security, it helps to know about these. Your web browser, for instance, connects to port 80 to send and receive HTTP traffic. Here are the common ports and precautions on their use:

PORT	SERVICE	USES AND ABUSES
7	Echo	Used by the ping command to determine whether a computer is responding. A hacker may use this to determine if there's a PC at a particular address.
21	FTP	For transferring files. Poor security means you should never have FTP visible to the internet.
23	Telnet	For remote logins on Linux and UNIX computers. This is particularly useful for testing potential passwords.
25/110	SMTP/POP3	Simple Mail Transport Protocol and Post Office Protocol 3. A poorly configured mail server allows a hacker to find usernames, exploit vulnerabilities in the mail server software and possibly even send mail anonymously.
80	HTTP	World Wide Web. Simple requests for information can reveal a lot more about the server than you bargained for, so it pays to keep your web server up to date.
137-139	NetBIOS	These ports indicate a Windows computer. Several utilities enable hackers to steal large amounts of information when these are open, including share names, usernames and even the groups to which users belong.
111/135	RPC	(Port 111 on Linux, port 135 on Windows) Remote Procedure Calls are a standard way of executing code on another system. Unfortunately, hackers can interrogate this service to find which RPC services are available, including version numbers. Some older service versions have vulnerabilities that can enable high-level access to the PC.
2301	Compaq	Some Compaq servers ship with a useful web-based management interface running on this port, rather than port 80. The default passwords are well known and access may enable you to see other internal computers and even shut them down or reconfigure them at will.

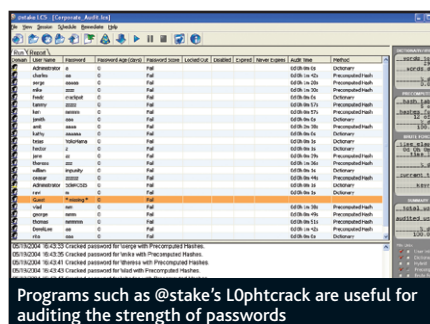
This list is by no means exhaustive, but utilities such as nmap can tell you the ports your systems have open. As a rule, close or block all ports you know you don't need at the firewall. This probably means leaving only mail and web ports open. Block all incoming connection requests, too. For a full list of ports and the services they provide, see www.iana.org/assignments/port-numbers.

L0phtcrack (www.atstake.com/products/lc) is a password cracker for Windows. Cracking passwords is remarkably useful. Losing the administrator password can mean having to reinstall Windows from scratch to reset it; L0phtcrack can help you recover lost passwords in a matter of minutes. It will also let you discover which users set their password to something simple so they can't forget it. In the Linux world, Crack 5.0a (www.crypticcode.com/users/alecm) is the tool of choice for breaking passwords. Written by Alec Muffet, Crack not only breaks passwords quickly but can also run in parallel across several systems for extra speed.

AUTOMATIC FOR THE PEOPLE

While learning hacking tricks is one way to secure your systems, it does take time and effort. The state of the art moves so quickly that it can become time-consuming just keeping up. An alternative is to use an automated security-testing tool.

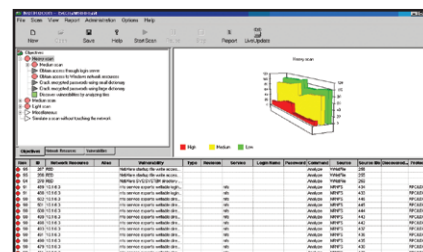
Automated tools don't just scan your network, they also probe them for a wide range of known vulnerabilities. Even better, some tools give you a detailed description of the problems discovered and tell you what to do about them. The problem many people have is in understanding what such tools tell you, so some knowledge of what the different ports are for and how to configure the software behind them is essential before you start, otherwise you may make a bad situation worse. There's also a tendency among certain automated tools to report false positives: problems where none exists. While it's better to be safe than sorry, you should be aware of this.



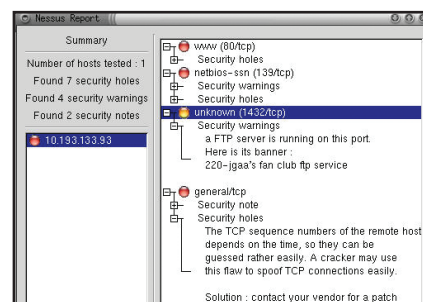
Programs such as @stake's L0phtcrack are useful for auditing the strength of passwords

Of the free security scanners available, Nessus is a long-established open-source tool available for Windows and Linux. Nessus, which is used in more than 75,000 organisations worldwide, benefits from regular updates to its database of tests. Free plug-ins address each type of attack, making Nessus extendable when new threats appear. Nessus is safe to use. But as its website says, it also enables you to "throw everything you can at a remote host to see how well it withstands attacks from intruders."

There are also sophisticated commercial vulnerability scanners available. NetRecon (<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=46>) by network security experts Symantec is one well-established offering. As well as checking for a wide range of vulnerabilities, this scanner simulates common intrusion techniques to gather evidence on how vulnerable your network is. NetRecon also uses Symantec's Live Update technology to keep itself automatically updated with newly discovered intrusion techniques and vulnerabilities to check.



Commercial security scanners such as Symantec's NetRecon update themselves automatically to counter new threats as they emerge



Automated security scanners such as Nessus can find network security problems quickly, but you should beware of false positives

As well as scanning for known vulnerabilities, it's worth installing a system to watch for unusual network activity that may indicate the attentions of a hacker. Intrusion detection systems monitor network activity looking for any telltale attack signatures. Snort (www.snort.org) is probably the best known and has the advantage of being free. Commercial applications include Tripwire (www.tripwire.com), which sits on specific servers and monitors changes in the software and data configuration. There are also dedicated hardware appliances such as the Proventia system (www.securehq.com/group.wml&deptid=73&groupid=407) that simply plug into your network.

PROFESSIONAL HELP

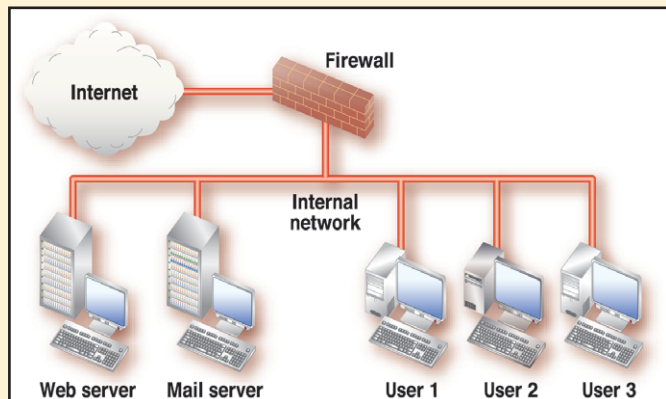
For an increasing number of people, the best way to secure their network is to rent the talents of a professional security consultant. This approach solves the problem of having to learn about and keep abreast of network security issues. But such expertise comes at a price. The job of such a consultant is to go through the same detailed procedures and careful techniques as a malicious hacker, but without the evil intent.

When the consultant is finished, you should receive a full report detailing the security problems he encountered and what to do about them. Some even provide a seminar in which to discuss the best approach to any serious security holes and the consultant himself may be able to perform any remedial work for you as well as recommending products and giving advice that will help keep you secure in future.

It's important to check that the person or company you choose doesn't simply use an automated security scanner and present you with its output. You should always ensure that it performs its own battery of manual tests and that it has reference sites you can check. Most companies will also provide you with sample analysis reports showing what you can expect from their service. For more details, see the 'Meet the Professionals' box opposite.

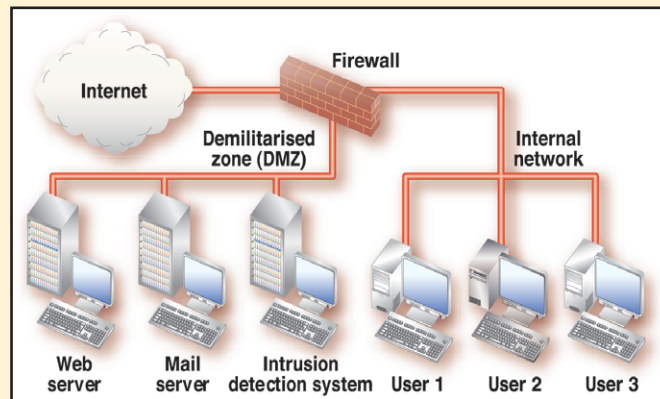


KEEP YOUR INTERNAL NETWORK SECURE



In the network configuration on the left, the system administrator has opted to put his internet-facing servers and his users on one internal network, protected by a firewall. But if the mail server or web server is compromised, it will serve as a stepping stone to the rest of the network.

In the configuration on the right, the administrator has put the mail and web servers on their own network – this is called a demilitarised zone



or DMZ – backed by an intrusion detection system. If the DMZ is hacked, the internal network remains secure and the DMZ's intrusion detection system should warn you. The firewall controls all traffic between the internal network, the DMZ and the internet. The firewall allows web browsing from the internal network. The intrusion detection system on the internal network gives early warning of any unwelcome activity.

CHECKS AND BALANCES

If you don't employ a professional network security consultant or learn to hack your own network, there are still steps you can take to maintain a level of security that will encourage hackers to find another target.

First, look at the amount of information you expose. If you own a domain, think about personal information such as email addresses used in the registration records and the passwords used to secure those accounts. If you have permanent IP addresses, you'll probably have a DNS record too. Have you named your internet-facing computers to reflect their function? If so, you could give a potential attacker a head start. Renaming them to, say, your favourite cartoon characters or similar will

make a hacker's job far more difficult, forcing them to probe your systems directly.

To catch a hacker in the act, install an intrusion detection system. The ability to detect suspicious activity will give you a valuable early warning. If needs be, you can always pull the plug on your internet link. Similarly, it's a wise idea to reorganise your network so internet-facing servers sit in their own 'demilitarised zone' (DMZ), separate from the main network, with access controlled by a third interface on your firewall. The diagram above shows you how to tackle this.

If you run your own DNS server, ensure you configure it so that zone transfers are not possible for anyone who requests them. As the 'Hacking the CIA' box explains, a zone transfer is a list of all PCs

on your domain that the DNS server knows about. For larger networks, these can contain large amounts of useful information for an attacker.

The computers that face the internet should have open only the ports they need. Your firewall should filter out all requests to connect to any others. Also, keep your firewall patched and up to date. From time to time it may be necessary to use File Transfer Protocol (FTP) or Telnet over the internet. If you need to use these services, allow such traffic through your firewall only as and when you need access. If you need to use insecure protocols such as FTP over the internet regularly, you should use encryption in the form of a virtual private network (VPN) or secure shell (SSH). Free versions of SSH exist for Windows and Linux at www.openssh.com.

You should also remember to install service and security patches as they become available. There's a window of opportunity from when a new flaw becomes public to when working exploits appear. Your job is to make sure the window slams shut before the first exploits appear.

To find out the vulnerabilities in the specific versions of the operating systems and programs you run, visit the Security Focus vulnerability database at www.securityfocus.com/bid. This contains detailed information about software flaws. Subscribing to the associated Bugtraq mailing list will give you early warning of new vulnerabilities. It isn't just people who exploit newly discovered vulnerabilities; by applying patches as they become available, you'll also keep yourself safe from worms and other automated nastiness.

TESTING TIMES

Security is an ongoing process, but there's a well-trodden path of discovery leading from finding a network to hacking into it. Even implementing some basic security measures can be enough to frustrate a hacker's ambitions. Hacking looks likely to remain a fact of online life, but if you can indicate clearly to an intruder that you've taken precautions it may be enough to make him move on to easier targets. **CS**

MEET THE PROFESSIONALS

Many companies will help you protect your network against hackers. We talked to John Pringle of Crewe-based Boldon James to find out more. First we asked why people who understand the importance of network security keep putting it off. "People become complacent," he said. "Good intentions go by the wayside with conflicting demands on time and effort. Also, as computers become more user-friendly, there is less need to have pure technicians doing the back-room stuff."

System administrators and people who run their own networks can learn about security from the internet or books, so what more can a professional network security consultant provide? "External consultants generally have a greater breadth and depth of knowledge and skill," Pringle said. "You may undertake a security health check once, but external specialists do it all the time."

If you're planning to hire someone to assess your network, there are a few things to bear in mind. "You need to have confidence that they understand what you want and

won't try to impose their preferred solution," cautioned Pringle. "Also, check references, preferably from a similar-sized, technically comparable organisation."

Some people worry that by having a third party assess their network, they are opening the door to a hacker in a suit. "CESG, the UK's national technical authority, has very good schemes designed to give you confidence in individuals and companies," Pringle said. "The CHECK scheme is a company-based scheme for technical vulnerability assessments and penetration testing. Members have to abide by a code of conduct. They have undergone a range of security clearances and their work is subject to independent review by CESG."

He added, "It does wonders for peace of mind to have a trusted third party give you an independent assessment that things are OK. Often the result of such advice is not to spend vast sums on security products, but simply to apply common sense procedures."

To find out more about the government's CHECK scheme, visit www.cesg.gov.uk.